PCT/IB04/ 51378 PHDE030285 GP

Europäisches Patentamt | European Patent Office | Office européen des brevets

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. | Patent application No. | Demande de brevet n°

03102524.0

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr:
Application no.: 03102524.0
Demande no:

Anmeldetag:
Date of filing: 13.08.03
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Philips Intellectual Property & Standards
GmbH
Steindamm 94
20099 Hamburg
ALLEMAGNE
Koninklijke Philips Electronics N.V.
Groenewoudseweg 1
5621 BA Eindhoven
PAYS-BAS

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Verschlüsselungs-Verfahren und Entschlüsselungs-Verfahren für ein digitales Übertragungssystem

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

H04L9/12

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL
PT RO SE SI SK TR LI

BESCHREIBUNG

VERSCHLÜSSELUNGS-VERFAHREN UND ENTSCHLÜSSELUNGS-VERFAHREN FÜR EIN DIGITALES ÜBERTRAGUNGSSYSTEM

Die Erfindung betrifft sowohl ein Verschlüsselungs-Verfahren, als auch ein Entschlüsselungsverfahren für ein digitales Übertragungssystem, welches aus einem Sender und einem Empfänger besteht, wobei die Übertragung alternativ schnurlos oder leitungsgebunden erfolgen kann. In einem digitalen Kommunikationssystem müssen die Empfänger auf die moduliert einkommenden Symbole synchronisiert werden, um eine optimale Demodulation zu erreichen. Für Mehrband-Modulations-Systeme und insbesondere für das Mehrträgerverfahren OFDM (im Englischen "Orthogonal Frequency Division Multiplex") ist die Frequenzsynchronisation wichtig. Fehler in der Zeitzählung (Timing) oder Abweichungen in der Frequenz (Frequency Offsets) führen dem Übertragungssystem Zwischenträgerstörungen (Inter Carrier Interference = ICI) und Intersymbolstörungen (Inter Symbol Interference = ISI) zu, wodurch eine Demodulation des Symbols nicht mehr möglich ist.

Ein bekanntes Verfahren zur Synchronisation ist die Data Aided Synchronisation. Das Prinzip dieses Synchronisations-Verfahrens ist, Lern-Sequenzen (Training Sequences) oder Pilotträger (Pilot Subcarriers) mit Bezugssymbolen zu verwenden, welche sowohl im Sender als auch im Empfänger hinterlegt sind. Dabei wird zum einen die Lern-Sequenz aus dem abgetasteten Empfangssignal herausgezogen und einem Korrelator zugeführt, zum anderen wird die im Empfänger gespeicherte Referenz-Sequenz aufgerufen und ebenfalls dem Korrelator zugeführt. Auf Basis des von dem Korrelator gefundenen Maximums wird der Abtaster für die zeitlich gerasterte Abfrage des Empfangssignals dahingehend gesteuert, dass Sender und Empfänger möglichst synchron sind. Das Korrelieren der empfangenen Lern-Sequenz mit der hinterlegten Referenz-Sequenz ermöglicht die Abschätzung der zeitlichen Lage des Symbols (Symbol Timing) bzw. der Frequenzabweichung.

In Figur 1 zum Stand der Technik ist schematisch ein digitaler Datenstrom r dargestellt,

der aus einer sich abwechselnden Folge (Sequenz) von Referenz-Symbolen einer Lern-Sequenz c und Daten-Symbolen s besteht. Die Lern-Sequenz c weist Referenz-Symbole auf, welche sowohl im Sender, als auch im Empfänger hinterlegt sind und beispielsweise eine Sequenz von aufeinanderfolgenden Bits mit konstanter Länge sein können. Als Lern-Sequenz werden üblicherweise von Zufallsgeneratoren erzeugte Codes verwendet.

Das grundlegende Verfahren zur Synchronisation ist in den Teilfiguren 2a) und 2b) zum Stand der Technik dargestellt. Teilfigur 2a) zeigt das Einfügen der Datensymbole s mit dem konstanten Code c. Daraus entsteht der zu sendende digitale Datenstrom r.

In Teilfigur 2b) wird aus dem empfangenen Datenstrom r die Lern-Sequenz mit dem Vektor c herausgezogen. Dieser wird mit dem im Empfänger abgelegten oder erzeugten Referenz-Sequenz c verglichen. Wenn ein Maximum gefunden ist, wird die Steuerung des Symboltaktes und die zeitliche Lage des Symbols des Empfängers entsprechend an die des Senders angepaßt und somit die Frequenzabweichung möglichst ausgeglichen. Die Referenz-Sequenz bzw. die Lern-Sequenz c besteht dabei aus einem Vektor mit einer Anzahl P von Referenz-Symbolen. Der Vektor wird dabei durch die folgende Gleichung (1) beschrieben:

$$c = [\, c_0 \;\; c_1 \;\; C \;\; c_{(P-1)} \,]^T \qquad (1)$$

Dieses Verfahren kann sowohl im Zeitbereich für das Symboltiming, als auch im Frequenz-Bereich für die Frequenz-Abschätzung durchgeführt werden. Es ist hier stellvertretend beschrieben für Systeme, die eine datenunterstützte Synchronisation verwenden.

Der Vektor c bleibt während der Dauer einer Verbindung konstant. Dies ermöglicht einem unberechtigten Dritten, ein Gerät bezüglich der bestehenden Verbindung zu synchronisieren, beispielsweise durch testweises Ausprobieren unterschiedlicher Codes. Ein unberechtigter Dritter könnte also mit geeigneten Mitteln die Verbindung abhören.

Aufgabe der Erfindung ist es daher, für ein gattungsgemäßes digitales Übertragungssystem ein Verfahren zum Verschlüsseln des digitalen Datenstroms anzugeben, welches die Abhörsicherheit des Datenstroms erhöht. Des weiteren ist es Aufgabe der Erfindung, ein Verfahren zum Entschlüsseln eines verschlüsselt gesendeten digitalen Datenstroms anzugeben. Es ist ferner Aufgabe der Erfindung, eine Vorrichtung zum Durchführen eines solchen Verfahrens anzugeben. Es ist außerdem Aufgabe der Erfindung, ein digitales Übertragungssystem anzugeben, dessen Abhörsicherheit erhöht ist.

Das Verschlüsselungs-Verfahren für ein digitales Übertragungssystem betreffend wird die Aufgabe gelöst durch ein Verfahren, bei dem der digitale Datenstrom aus einer sich abwechselnden Folge von Lern-Sequenzen oder Pilotträgern (im folgenden lediglich Lern-Sequenzen bezeichnet) und Daten-Symbolen besteht und die Lern-Sequenz codiert übertragen wird und zwar derart, dass die Codierung der Lern-Sequenz mit einem dynamischen Verschlüsselungs-Code erfolgt. Dynamisch bedeutet in diesem Zusammenhang, dass die Lern-Sequenz, die durch einen Vektor mit bestimmter Länge gebildet wird, im Laufe der Zeit unterschiedlichen Inhalt hat. Dies bedeutet, dass während einer Übertragung sich der Inhalt der Lern-Sequenz ändert, wodurch die Abhörsicherheit erhöht und ein Verschlüsselungsgrad erreicht wird.

Nach einer Ausführungsform der Erfindung wird der dynamische Verschlüsselungs-Code von einem Zufallsgenerator erzeugt.

Einer andere Ausführungsform verwendet für das Verschlüsselungsverfahren nacheinander einzelne Elemente eines definierten Satzes von Verschlüsselungs-Codes. Dieser definierte Satz von Verschlüsselungs-Codes kann beispielsweise vorab von dem Zufallsgenerator erzeugt sein oder bei der Herstellung der korrespondierenden Vorrichtung programmiert worden sein.

Nach einer weiteren Ausführungsform der Erfindung sind die dynamischen Lern-

Sequenzen einzelne Elemente eines Satzes von Lern-Sequenzen und werden nacheinander angewandt. Dieser Satz von Lern-Sequenzen kann dabei alternativ
- übertragen werden vom Sender zum Empfänger und von diesem (zwischen-) gespeichert werden oder
- nach einem definierten Muster vom Empfänger erzeugt werden, und zwar im voraus und mit anschließender Zwischenspeicherung oder zeitnah (just in time) zur Verwendung.

Nach einer anderen Ausführungsform wird der Satz von dynamischen Lern-Sequenzen im Sinne einer Schleife von Anfang bis Ende und anschließend wieder am Anfang beginnend durchlaufen. Dadurch wird sichergestellt, dass jede einzelne Lern-Sequenz nur für eine bestimmte Zeit angewandt wird und bei länger andauernden Datenübertragungen nicht doch ein quasi statischer Zustand der Codierung erreicht würde, dadurch, dass das letzte Element der Lern-Sequenz dauerhaft verwendet würde. Bei diesen Ausführungsformen werden die Lern-Sequenzen gleichzeitig auf der Senderseite und der Empfängerseite geändert. Die Zeitpunkte, zu denen die Lern-Sequenzen geändert werden, sind Sender und Empfänger bekannt, und beim Aufbau der Verbindung zwischen Sender und Empfänger vereinbart worden.

Das Entschlüsselungs-Verfahren betreffend wird die Aufgabe gelöst durch ein Verfahren für einen digitalen Datenstrom, der von einem Abtaster ermittelt wird und aus einer sich abwechselnden Folge von Lern-Sequenzen und Daten-Symbolen besteht, wobei die Lern-Sequenzen codiert sind und nach dem Abtasten des empfangenen digitalen Datenstroms aus diesem extrahiert und einem Korrelator zugeführt werden und ein empfängerseitiger Entschlüsselungs-Code ebenfalls dem Korrelator zugeführt wird, welcher auf Basis der beiden Signale ein Maximum findet, welches als Stellgröße für die Zeit- bzw. Frequenz-Korrektur des Abtasters verwendet wird, und wobei der Entschlüsselungs-Code dynamisch ist und ein Code-Generator den dynamischen Entschlüsselungs-Code in Abhängigkeit von einem Encryption Key erzeugt. Da sich der Entschlüsselungs-Code mit der Zeit ändert, also dynamisch ist, wird die Abhörsicherheit erhöht. Der Code-Generator erzeugt den dynamischen

Entschlüsselungs-Code in Abhängigkeit von dem Inhalt eines Encryption Keys, welcher zu Beginn der Datenübertragung übermittelt wurde, und welcher Angaben beinhaltet, die für die Erzeugung des dynamischen Codes erforderlich sind. Das Ergebnis der Korrelation stellt ein Maß für den Zeit- bzw. Frequenz-Versatz zwischen Sender und Empfänger dar.

Nach einer Ausführungsform der Erfindung definiert eine Permutations-Funktion den Inhalt eines Satzes von Entschlüsselungs-Codes. Ein Satz enthält mehrere Entschlüsselungs-Codes, die von einer Permutations-Funktion quasi zufällig zusammengestellt werden, wobei die Permutations-Funktion auf eine vorgegebene Menge (einen Pool) von Entschlüsselungs-Codes zurückgreift. Da die einzelnen Entschlüsselungs-Codes des Pools immer wieder in einer anderen Reihenfolge zusammengestellt werden können, gibt es eine relativ große Menge von möglichen, zusammengesetzten Sätzen von Entschlüsselungs-Codes bei einem relativ geringen Bedarf an Speicherplatz.

Nach einer weiteren Ausführungsform der Erfindung enthält das Entschlüsselungs-Verfahren die Schritte:

- Übermitteln eines Encryption Keys und dadurch:
  - -- Festlegen einer Permutations-Funktion,
  - -- Festlegen eines Satzes von Entschlüsselungs-Codes,
  - -- Festlegen eines Sprung-Intervalls,

wobei die letztgenannten drei Schritte in beliebiger Reihenfolge durchgeführt werden können. Die Permutations-Funktion legt fest, in welcher Reihenfolge bestimmte Entschlüsselungs-Codes aus einem Pool herausgenommen werden und in einem Satz von Entschlüsselungs-Codes abgelegt werden. Das Sprung-Intervall gibt an, nach welcher Anzahl von Datenpaketen bzw. nach welcher Zeitdauer der Wechsel zum nächsten Entschlüsselungs-Code stattfindet.

Nach einer Variante der Erfindung wird ein Permutations-Ablauf durchgeführt, der eine Schleife mit folgenden Schritten beinhaltet:

- Setzen eines Intervalls auf 1;
- Abwarten des Endes eines vordefinierten Sprung-Intervalls;
- Erhöhen des Intervalls um den Wert 1;
- Durchführen eines Vergleichs, ob der aktuelle Wert des Intervalls größer ist als die gesamte Anzahl der Elemente einer Permutations-Funktion, welche die Positionen der für eine Entschlüsselung des digitalen Datenstroms zu verwendenden dynamischen Codes angibt,

wobei alternativ erfolgt, wenn der Vergleich positiv ausgeht:

- Zurücksetzen des Intervalls auf den Wert 1,

und wenn der Vergleich negativ ausgeht:

- Gleichsetzen der augenblicklichen Entschlüsselungs-Funktion mit dem Entschlüsselungs-Code, der dem Code der von der Permutations-Funktion vorgegebenen Position entspricht.

Dieser Permutations-Ablauf sieht vor, dass ein einzelner Entschlüsselungs-Code für die Zeitdauer eines Intervalls angewandt wird und anschließend von einem anderen Entschlüsselungs-Code abgelöst wird.

Zusammengefaßt wird die Abhörsicherheit erhöht durch zeitliches Verändern des Codes, wobei je nach Variante der Erfindung unterschiedliche Verschlüsselungsgrade erreicht werden. Dabei können die Maßnahmen

1) Verwenden eines Satzes unterschiedlicher Verschlüsselungs-Codes,
2) Verwenden einer Permutations-Funktion und/oder
3) Verwenden eines Sprung-Intervalls, das für unterschiedliche Verbindungen unterschiedlich lang ist

einzeln oder in Verbindung miteinander angewandt werden. Je mehr Maßnahmen realisiert werden, desto höher ist die Komplexität und somit der Verschlüsselungsgrad. Die Komplexität wird weiter erhöht durch Verwenden von Faktoren größeren Inhalts und somit durch größere Abwechslung.

Die Erfindung wird in der physikalischen Schicht des OSI-7-Schichten Modells angewandt.

Die Vorrichtung betreffend wird die Aufgabe gelöst durch eine Vorrichtung für die Synchronisation eines Empfängers auf einen empfangenen digitalen Datenstrom, wobei für die Durchführung der Synchronisation aus dem empfangenen Datenstrom Lern-Sequenzen extrahiert werden und einem Korrelator zugeführt werden, wo sie mit einem Entschlüsselungs-Code, dem Referenzcode, gemischt werden, um ein Maximum zu finden, welches als Stellgröße für einen Abtaster verwendet wird und wobei die Synchronisations-Vorrichtung einen dynamischen Code-Generator aufweist. Der dynamische Code-Generator erzeugt alternativ den Entschlüsselungs-Code, der aktuell gebraucht wird, oder er erzeugt einen ganzen Satz von Entschlüsselungs-Codes und hinterlegt sie in einem Speicher.
Innerhalb einer Vorrichtung, bspw. einem (Mobil-) Funktelefon kann der dynamischen Generator zum Verschlüsseln beim Senden und zum Entschlüsseln beim Empfang eingesetzt werden.

Nach einer Ausführungsform der Erfindung weist die Synchronisations-Vorrichtung Mittel zum Speichern des Encryption Keys auf, beispielsweise ein RAM (Random Acces Memory).

Bezüglich des Übertragungssystems wird die Erfindung gelöst durch ein digitales Übertragungssystem mit einer Vorrichtung für die Synchronisation eines Empfängers auf einen empfangenen digitalen Datenstrom, bei dem der Empfänger
- Mittel für die Extraktion von Lern-Sequenzen,
- Mittel zum Ermitteln einer Stellgröße für einen Abtaster und
- Mittel zum Erzeugen eines dynamischen Codes

aufweist.
Die Stellgröße für den Abtaster wird beispielsweise von einem Korrelator ermittelt. Sie beeinflußt den Abtaster dahingehend, dass der Zeit- bzw. der Frequenz-Versatz zwischen Sender und Empfänger verringert wird. Das Mittel zum Erzeugen eines dynamischen Codes ist beispielsweise ein Code-Generator, der für jede Verbindung nach Maßgabe des Encryption Keys die mehreren zu verwendenden Entschlüsselungs-

Codes erzeugt.

Verwendung eines Verschlüsselungs-Verfahrens und/oder eines Entschlüsselungs-Verfahrens, bei dem der digitale Datenstrom aus einer sich abwechselnden Folge von Lern-Sequenzen und Daten-Symbolen besteht und die Lern-Sequenzen dynamisch codiert sind, in leitungsgebundenen oder schnurlosen Netzwerken wie beispielsweise einem Telekommunikationsnetz oder einem WirelessLAN (Local Area Network).

Im folgenden wird die Erfindung lediglich beispielhaft anhand der folgenden Zeichnungen erläutert, wobei

Figur 3 schematisch einen digitalen Datenstrom mit dynamisch veränderten Lern-Sequenzen darstellt,

Figur 4 in den Teilfiguren a) und b) schematisch ein Ablaufdiagramm für die Synchronisation eines Empfängers auf einen empfangenen dynamisch verschlüsselten Datenstrom zeigt,

Figur 5 ein Ablaufdiagramm für ein Entschlüsselungs-Verfahren und

Figur 6 einen Pool von einzelnen Codes zeigt.

Figur 3 zeigt schematisch einen digitalen Datenstrom x(t), der aus einer sich abwechselnden Folge von dynamisch veränderten Lern-Sequenzen v_n, v_{n+1} und Datensymbolen u besteht. Eine Lern-Sequenz v_n oder v_{n+1}wird codiert übertragen. Dadurch, dass hier im Verlauf der Übertragung der Code geändert wird, wird ein erster Verschlüsselungsgrad erreicht. Codierung meint in diesem Zusammenhang, dass für die Dauer der Übertragung ein und derselbe Code verwendet wird. Verschlüsselung meint in diesem Zusammenhang, dass für die Dauer der Übertragung zumindest zwei unterschiedliche Codes verwendet werden.

Bei diesem Ausführungsbeispiel mit einem Sprung-Intervall, das kürzer ist als die Dauer der Datensymbole, wird zumindest für zwei aufeinanderfolgende Lern-Sequenzen ein unterschiedlicher Code verwendet, angedeutet durch v_n und v_{n+1}. Beide Codes v_n, v_{n+1} bestehen aus derselben Anzahl P von Referenz-Symbolen, die für die

Synchronisation verwendet wird. Jeder Code v_n, ... v_{n+1} weist dieselbe Anzahl P von Referenz-Symbolen auf, die Referenz-Symbole selber unterscheiden sich jedoch. Andere Varianten wechseln den Code nach einer höheren Anzahl von Datensymbolen oder nach Ablauf einer vorbestimmten Zeit.

Teilfigur 4a) zeigt das Mischen der im Sender erzeugten Datensymbole u mit dem zeitlich veränderten Verschlüsselungs-Code v(t). Das Ergebnis ist der digitale Datenstrom x(t).

Teilfigur 4b) zeigt ein Ablaufdiagramm für die Synchronisation des Empfängers auf den empfangenen Datenstrom x(t). Das Abtasten des empfangenen Datenstroms x(t) erfolgt zeitabhängig. Um ein möglichst optimales Ergebnis zu erzielen, ist es wichtig, dass der Zeit- bzw. der Frequenz-Versatz zwischen der lokalen Uhr des Senders und der lokalen Uhr des Empfängers gering ist. Nach Extraktion einer Lern-Sequenz v_n wird diese einem Korrelator zugeführt, wo sie mit dem Referenz-Signal v_n des Empfängers verglichen wird. Das Ergebnis der Korrelation wird auf ein Maximum hin untersucht, welches als Stellwert für das Angleichen des Abtasters verwendet wird. Das hier beschriebene Synchronisations-Verfahren kann als dynamisch beschrieben werden, da der Code für die Verschlüsselung der Lern-Sequenzen sich mit der Zeit ändert. Ein dynamischer Code-Generator erzeugt nach Maßgabe eines Encryption Keys die empfängerseitige Vergleichs-Lern-Sequenz v_n, nämlich das Referenz-Signal. Die Variable (t) soll verdeutlichen, dass der Verschlüsselungs-Code v(t) sich mit der Zeit ändert, also dynamisch ist. Der Index n steht jeweils für einen bestimmten augenblicklichen Verschlüsselungs-Code v_n, welcher abgelöst wird von dem nächsten augenblicklichen Verschlüsselungs-Code v_{n+1}.

Figur 5 stellt in einem Ablaufdiagramm schematisch ein erfindungsgemäßes Verfahren zum Synchronisieren eines Empfängers eines digitalen Übertragungssystems auf den empfangenen digitalen Datenstrom x(t) dar. Im Anschluß an den Verbindungsaufbau 100 wird im Schritt 200 der Encryption Key übermittelt, der in beliebiger Reihenfolge das Festlegen folgender Parameter veranlaßt:

- einer Permutations-Funktion F_i 210;
- eines Satzes von Entschlüsselungs-Mustern G_i 220;
- eines Sprung-Intervalls I_{hop} 230.

Der Encryption Key 200 wird von der sendenden Einheit erzeugt und beinhaltet die für die Entschlüsselung des übertragenden Datensignals und für die Synchronisation erforderlichen Parameter.

Die Permutations-Funktion $F_i = \{p\_1, p\_2 \ldots p\_M\}$ gibt an, in welcher Reihenfolge die einzelnen Codes $g_1, g_2 \ldots g_H$ eines Satzes von G_i Verschlüsselungs-Mustern angewandt werden, dabei sind $p\_1, p\_2 \ldots p\_M$ beliebige ganze Zahlen 1, 2 ... H. Wenn eine bestimmte Permutations-Funktion beispielsweise lautet $F = \{2, H\}$, bedeutet dies, dass $p\_1 = 2$ und $p\_2 = H$ ist und beim Entschlüsseln zunächst der Verschlüsselungs-Code g_2 und anschließend der Verschlüsselungs-Code g_H angewandt wird. Sollte die Verbindung dann noch nicht beendet sein, wird das Entschlüsseln im Sinne einer Schleife fortgesetzt mit p_1, also g_2, und dann mit p_2, also g_H. Das Festlegen 210 der für die aktuelle Übertragung gültigen Permutations-Funktion kann alternativ erfolgen durch:

a) Übermitteln eines Vektors F_i, der die konkrete Permutations-Folge {p_1, p_2 ... p_M} beinhaltet oder
b) Übermitteln nur des Namens einer einzelnen Permutations-Funktion F_i.

Die Alternative a) ermöglicht einem unberechtigten dritten Teilnehmer die Permutations-Folge abzuhören und somit ein Hilfsmittel zum Entschlüsseln der Lern-Sequenz des gesendeten digitalen Datenstroms zu erhalten. Dieses Verfahren hat aber den Vorteil, dass sowohl senderseitig, als auch empfängerseitig Speicherplatz gespart wird, da die für die aktuelle Übermittlung gültige Permutations-Folge nur zwischengespeichert zu werden braucht und nach Beendigung der Übertragung gelöscht werden kann.

Die Alternative b) setzt voraus, dass sowohl senderseitig, als auch empfängerseitig alle möglichen Permutations-Funktionen F_1, F_2 ... F_L (L: ganzzahlig) dauerhaft gespeichert sein müssen, damit die für die Übertragung gültige Permutations-Funktion F_i aufgerufen werden kann. Vorteil dieser Variante ist, dass ein unberechtigter dritter Teilnehmer die hinter der verwendeten Permutations-Funktion F_i steckende Folge von Codes G_i nicht ermitteln kann, da sie nicht übermittelt wird.

Ein Satz G_i von Entschlüsselungs-Mustern beinhaltet H orthogonale Codes g_1, g_2 ... g_H, die geeignet sind, die Lern-Sequenz zu ändern. Jeder einzelne der H orthogonalen Codes v ist dabei als Vektor mit P-Elementen aufgebaut. Die Konstanten H und P sind ganzzahlig. Der Schritt des Festlegens eines Satzes G_i von Verschlüsselungs-Codes 220 kann alternativ erfolgen durch

entweder

c) Übermitteln der konkreten, einzelnen orthogonalen Codes g_1, g_2... in Form von Vektoren

oder

d) Übermittlung der Namen der anzuwendenden orthogonalen Codes.

Die Vor- und Nachteile der Alternativen c) und d) sind wie bei den Alternativen a) und b) beim Festlegen der Permutations-Funktion F_i die, dass das Übermitteln der konkreten Angaben die Abhörsicherheit verringert, dass das Speichern und Aufrufen vordefinierter Codes sowohl sender- als auch empfängerseitig Speicherplatz beansprucht.

Der Schritt 230 des Festlegens des Sprung-Intervalls I_{hop} bedeutet alternativ

entweder

e) Vorgabe einer Periodendauer T_{hop}, also einer zeitlichen Gültigkeitsdauer, beispielsweise 5 msec

oder

f) Vorgabe einer Anzahl Q von Datenpaketen, beispielsweise 3x Anzahl der

Datensymbole u.

Nach Übermittlung des Encryption Keys beginnt das dynamische Entschlüsseln 300. Der erste Permutations-Ablauf 400 ist der folgende. Bei Schritt 410 wird das Intervall n auf "1" gesetzt, derjenige Code aus dem Satz G_i wird verwendet, der an der Stelle p_1 der Permutations-Funktion F_i steht. Bei Schritt 420 wird der Ablauf des Sprung-Intervalls I_{hop} abgewartet. Das Messen der Zeit zum Ermitteln des Endes der Periodendauer bzw. das Zählen der übermittelten Datenpakete erfolgt durch entsprechende Vorrichtungen, wie beispielsweise einen Zähler oder einen Flip-Flop. Wenn das Ende des Sprung-Intervalls I_{hop} erreicht ist, wird in Schritt 430 das Intervall n um den Wert 1 erhöht. Bei Schritt 440 wird dann der Vergleich durchgeführt, ob der aktuelle Wert für das Intervall n größer ist, als die gesamte Anzahl M der Elemente des Permutations-Vektors. Ergibt der Vergleich "Ja", beginnt die Schleife wieder mit Schritt 410, und das Intervall n wird wieder auf "1" gesetzt. Ist das Ergebnis des Vergleichs „Nein", wird in Schritt 450 als augenblicklicher Entschlüsselungs-Code v_n derjenige aufgerufen, der an der n-ten Position p_n der Permutations-Funktion F_i steht, also $v_n = g_{(p\_n)}$ und solange angewandt, bis im Zuge der Schleife in Schritt 420 das Ende des Sprung-Intervalls I_{hop} erreicht ist und anschließend in Schritt 430 das Intervall n um den Wert "1" erhöht wird.

Fig. 6 zeigt einen Pool von p_1 Verschlüsselungs-Codes. Eine erste mit punktierter Linie eingezeichnete Teilmenge besteht aus 4 Elementen, die beispielhaft zu zwei möglichen Sätzen G_i zusammengesetzt sind. Insgesamt existieren 24 Möglichkeiten, wenn davon ausgegangen wird, dass jedes Element genau einmal vorkommt. Eine zweite mit gestrichelter Linie eingezeichnete Teilmenge umfaßt 5 Elemente. Hierfür sind ebenfalls zwei Möglichkeiten für Verschlüsselungs-Codes dargestellt, mit der Variante, dass einzelne Codes mehrfach vorkommen dürfen.

PATENTANSPRÜCHE

1. Verschlüsselungs-Verfahren für ein digitales Übertragungssystem, bei dem der digitale Datenstrom (x(t)) aus einer sich abwechselnden Folge von Lern-Sequenzen oder Pilotträgern und Datensymbolen (u) besteht und die Lern-Sequenz codiert übertragen wird, dadurch gekennzeichnet, dass die Codierung die Lern-Sequenz mit einem dynamischen Verschlüsselungs-Code (v_n) erfolgt.

2. Verschlüsselungs-Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der dynamische Verschlüsselungs-Code (v_n) von einem Zufallsgenerator erzeugt wird.

3. Verschlüsselungs-Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass das Verschlüsselungs-Verfahren nacheinander einzelne Elemente (v_n, v_{n+1} ...) eines definierten Satzes (G_i) von Verschlüsselungs-Codes anwendet.

4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, dass der Satz (G_i)von dynamischen Lern-Sequenzen (g_1, $g_{2...}$) im Sinne einer Schleife von Anfang bis Ende und anschließend wieder am Anfang beginnend durchlaufen wird.

5. Entschlüsselungs-Verfahren für einen digitalen Datenstrom (x(t)), der von einem Abtaster ermittelt wird und aus einer sich abwechselnden Folge von Lern-Sequenzen und Daten-Symbolen (u) besteht, wobei die Lern-Sequenzen oder Pilotträger codiert sind und nach dem Abtasten des empfangenen digitalen Datenstroms (x(t)) aus diesem extrahiert und einem Korrelator zugeführt werden und ein empfängerseitiger Entschlüsselungs-Code (v_n) ebenfalls dem Korrelator zugeführt wird, welcher auf Basis der beiden Signale ein Maximum findet, welches

als Stellgröße für die Zeit- bzw. Frequenz-Korrektur des Abtasters verwendet wird, dadurch gekennzeichnet, dass der Entschlüsselungs-Code (v_n) dynamisch ist und ein Code-Generator den dynamischen Entschlüsselungs-Code (v_n) in Abhängigkeit von einem Encryption Key (200) erzeugt.

6. Entschlüsselungs-Verfahren nach Anspruch 5, dadurch gekennzeichnet, dass eine Permutations-Funktion (F_i) den Inhalt eines Satzes von Entschlüsselungs-Codes (v_n) definiert.

7. Entschlüsselungs-Verfahren nach einem der Ansprüche 5 oder 6, gekennzeichnet durch die Schritte:
   - Übermitteln eines Encryption Keys (200) und dadurch:
     -- Festlegen (210) einer Permutations-Funktion (F_i),
     -- Festlegen (220) eines Satzes von Entschlüsselungs-Codes ($g_1, g_{2,...} g_H$),
     -- Festlegen (230) eines Sprung-Intervalls (I_{hop}),

   wobei die letztgenannten drei Schritte (210, 220, 230) in beliebiger Reihenfolge durchgeführt werden können.

8. Entschlüsselungs-Verfahren nach einem der Ansprüche 5 bis 7, gekennzeichnet durch das Durchführen eines Permutations-Ablaufs (400), der eine Schleife mit folgenden Schritten beinhaltet:
   - Setzen (410) eines Intervalls (n) auf 1;
   - Abwarten (420) des Endes eines vordefinierten Sprung-Intervalls (I_{hop});
   - Erhöhen (430) des Intervalls (n) um den Wert 1;
   - Durchführen eines Vergleichs (440), ob der aktuelle Wert des Intervalls (n) größer ist, als die gesamte Anzahl (M) der Elemente einer Permutations-Funktion (F_i), welche die Positionen der für eine Entschlüsselung des digitalen Datenstroms (x(t)) zu verwendenden dynamischen Codes (g_n) angibt, wobei alternativ erfolgt,

-- wenn der Vergleich positiv ausgeht: Zurücksetzen des Intervalls (n) auf den Wert 1;

-- wenn der Vergleich negativ ausgeht: Gleichsetzen der augenblicklichen Entschlüsselungs-Funktion (v_n) mit dem Entschlüsselungs-Code (g_{p_n}), der an der von der Permutations-Funktion (F_i) vorgegebenen Position (p_n) steht.

9. Vorrichtung für die Synchronisation eines Empfängers auf einen empfangenen digitalen Datenstrom, wobei für die Durchführung der Synchronisation aus dem empfangenen Datenstrom Lern-Sequenzen oder Pilotträger (v_n) extrahiert werden und mit dem Entschlüsselungs-Code korreliert werden, dadurch gekennzeichnet, dass die Synchronisations-Vorrichtung einen dynamischen Code-Generator aufweist.

10. Synchronisations-Vorrichtung nach Anspruch 9, dadurch gekennzeichnet, dass sie Mittel zum Speichern eines Encryption Keys (200) aufweist.

11. Digitales Übertragungssystem mit einer Vorrichtung für die Synchronisation eines Empfängers auf einen empfangenen digitalen Datenstrom, dadurch gekennzeichnet, dass der Empfänger
- Mittel für die Extraktion von Lern-Sequenzen,
- Mittel zum Ermitteln einer Stellgröße für einen Abtaster und
- Mittel zum Erzeugen eines dynamischen Codes aufweist.

12. Verwendung eines Verschlüsselungs-Verfahrens und/oder eines Entschlüsselungs-Verfahrens, bei dem der digitale Datenstrom aus einer sich abwechselnden Folge von Lern-Sequenzen oder Pilotträgern und Datensymbolen besteht und die Lern-Sequenz oder der Pilotträger dynamisch codiert ist, in leitungsgebundenen oder schnurlosen Netzwerken.

ZUSAMMENFASSUNG

VERSCHLÜSSELUNGS-VERFAHREN UND ENTSCHLÜSSELUNGS-VERFAHREN FÜR EIN DIGITALES ÜBERTRAGUNGSSYSTEM

Verschlüsselungs-Verfahren und Entschlüsselungs-Verfahren für ein digitales Übertragungssystem, bei dem der Datenstrom aus einer sich abwechselnden Folge von Lern-Sequenzen und Daten-Symbolen besteht und die Lern-Sequenzen dynamisch codiert werden. Empfängerseitig wird mittels eines Code-Generators in Abhängigkeit von einem Encryption Key (200) ein Entschlüsselungs-Code (v_n) erzeugt. Dieser Entschlüsselungs-Code wird einem Korrelator zugeführt, wo er mit dem aus dem digitalen Datenstrom extrahierten Verschlüsselungs-Code v_n gemischt wird. Der Korrelator erzeugt eine Stellgröße für den Ausgleich des Versatzes bezüglich der Zeit bzw. der Frequenz zwischen Sender und Empfänger. Eine Verschlüsselung wird durch das Ändern des während der Übertragung verwendeten Codes erreicht.

(Fig. 4)

Fig. 1

Stand der Technik

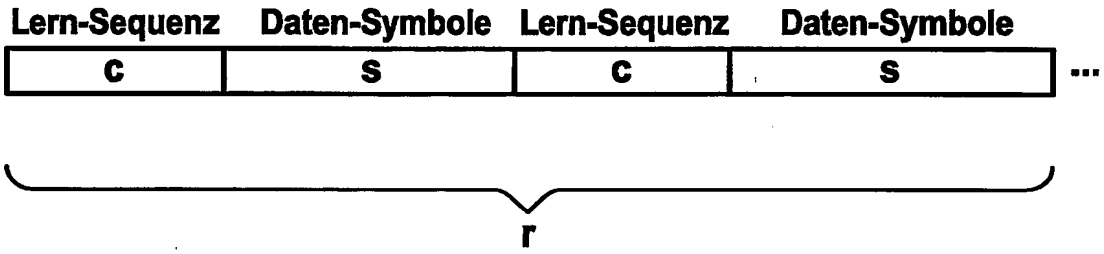


Fig. 2a)

Stand der Technik

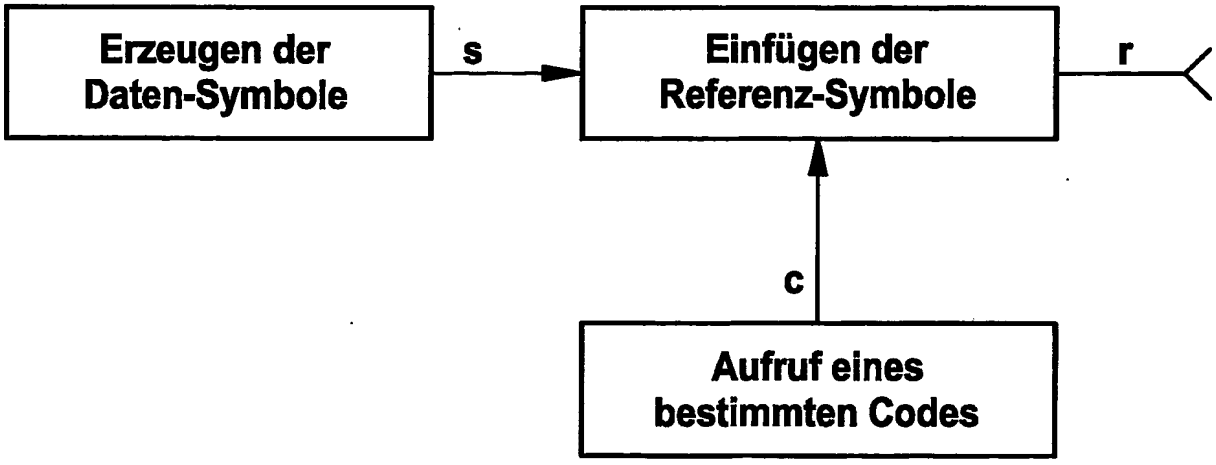


Fig. 2b)

Stand der Technik

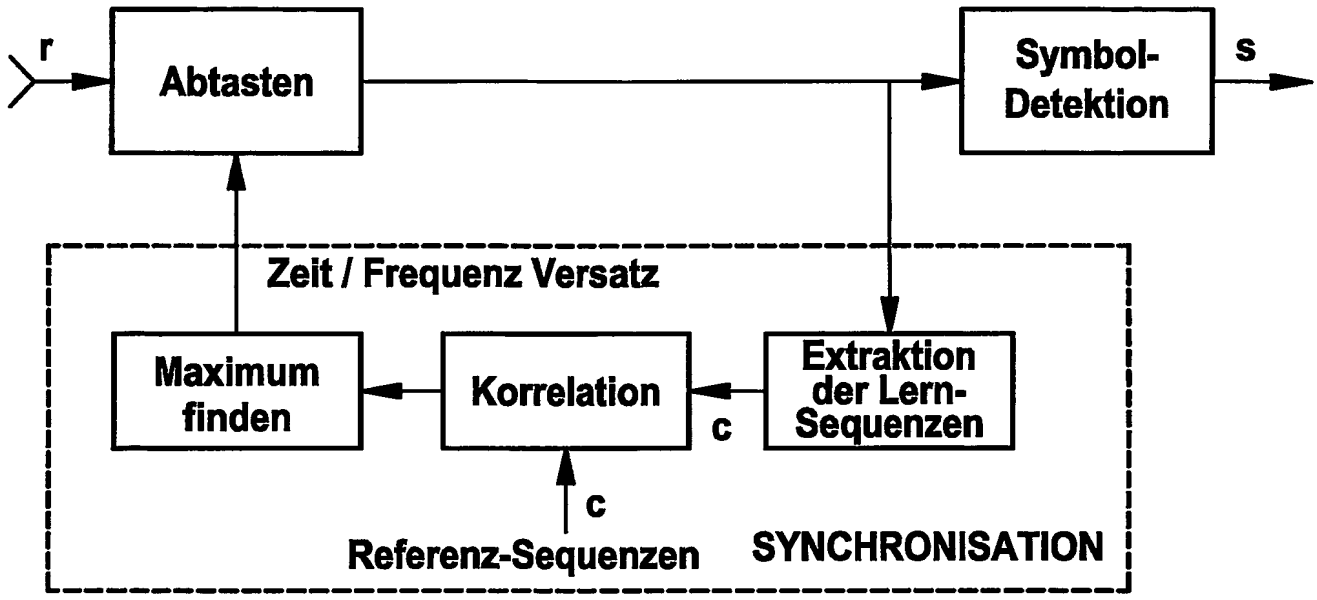


Fig. 3

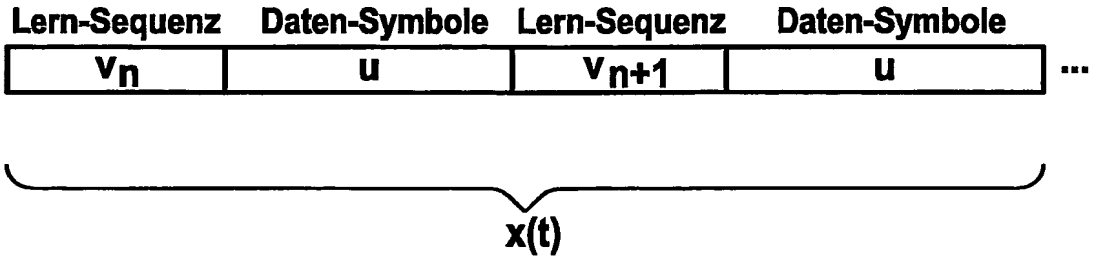


Fig. 4a)

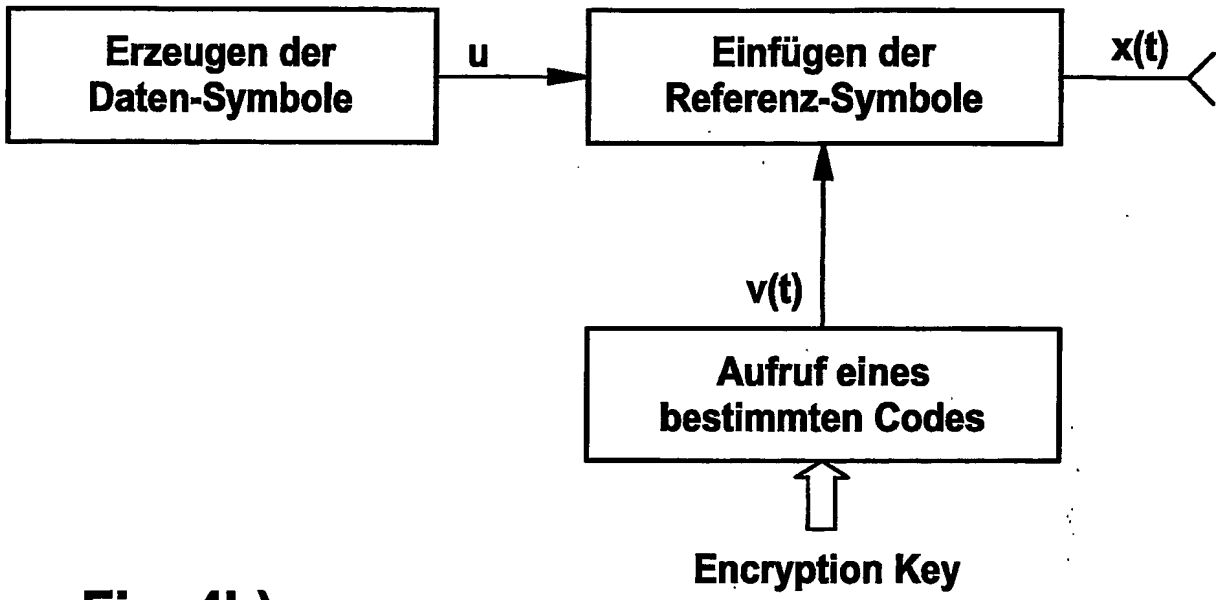

Erzeugen der Daten-Symbole
u
Einfügen der Referenz-Symbole
x(t)
v(t)
Aufruf eines bestimmten Codes
Encryption Key

Fig. 4b)

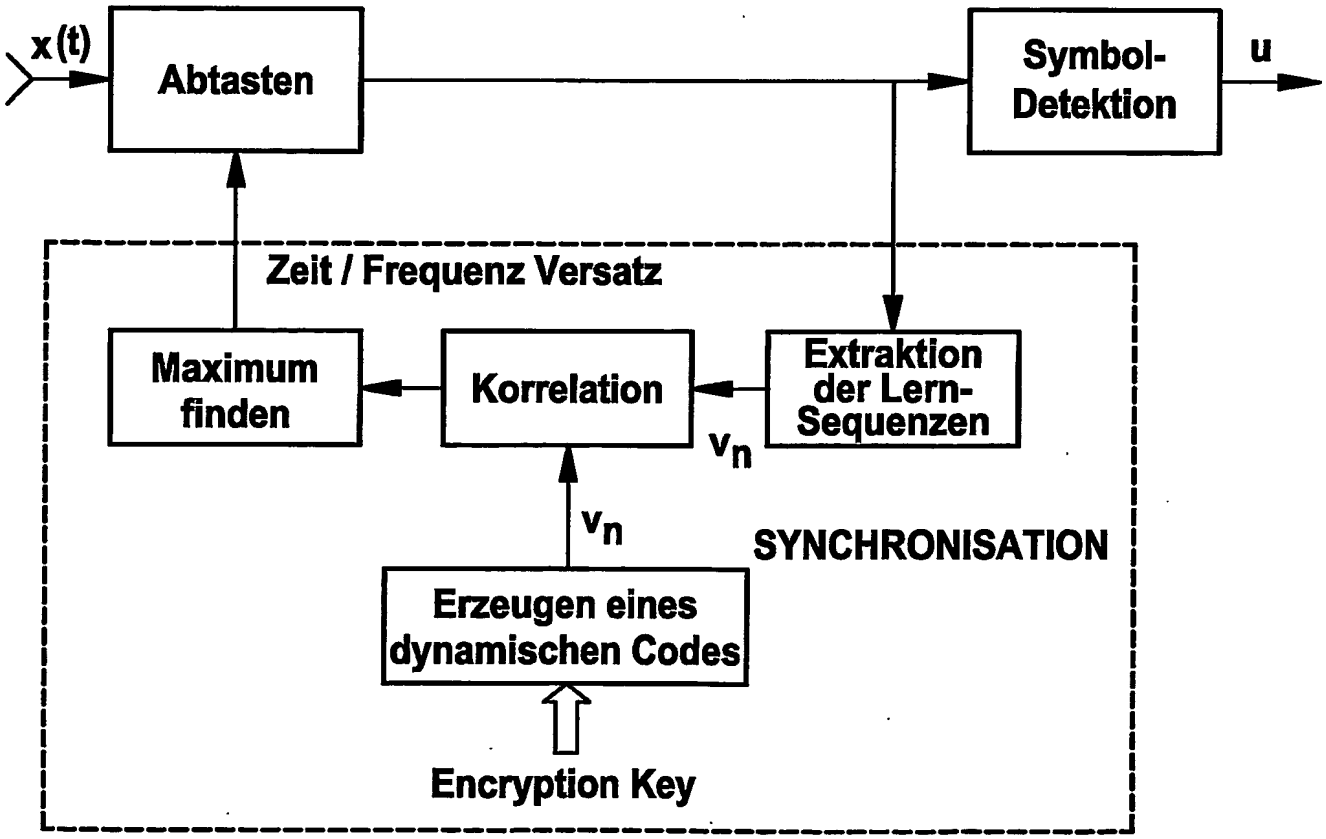

x(t)
Abtasten
Symbol-Detektion
u
Zeit / Frequenz Versatz
Maximum finden
Korrelation
Extraktion der Lern-Sequenzen
v_n
v_n
SYNCHRONISATION
Erzeugen eines dynamischen Codes
Encryption Key

Fig. 5

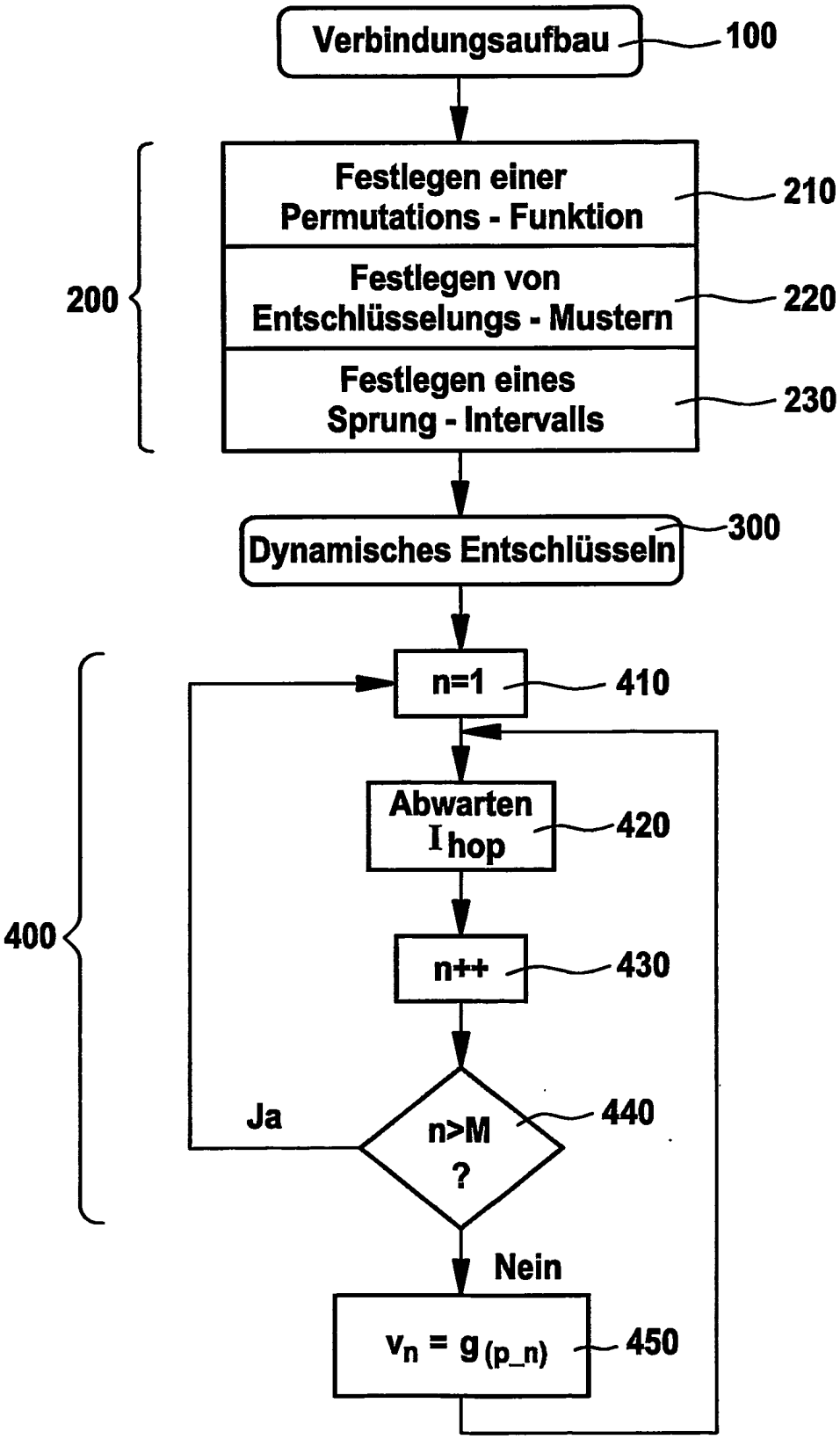
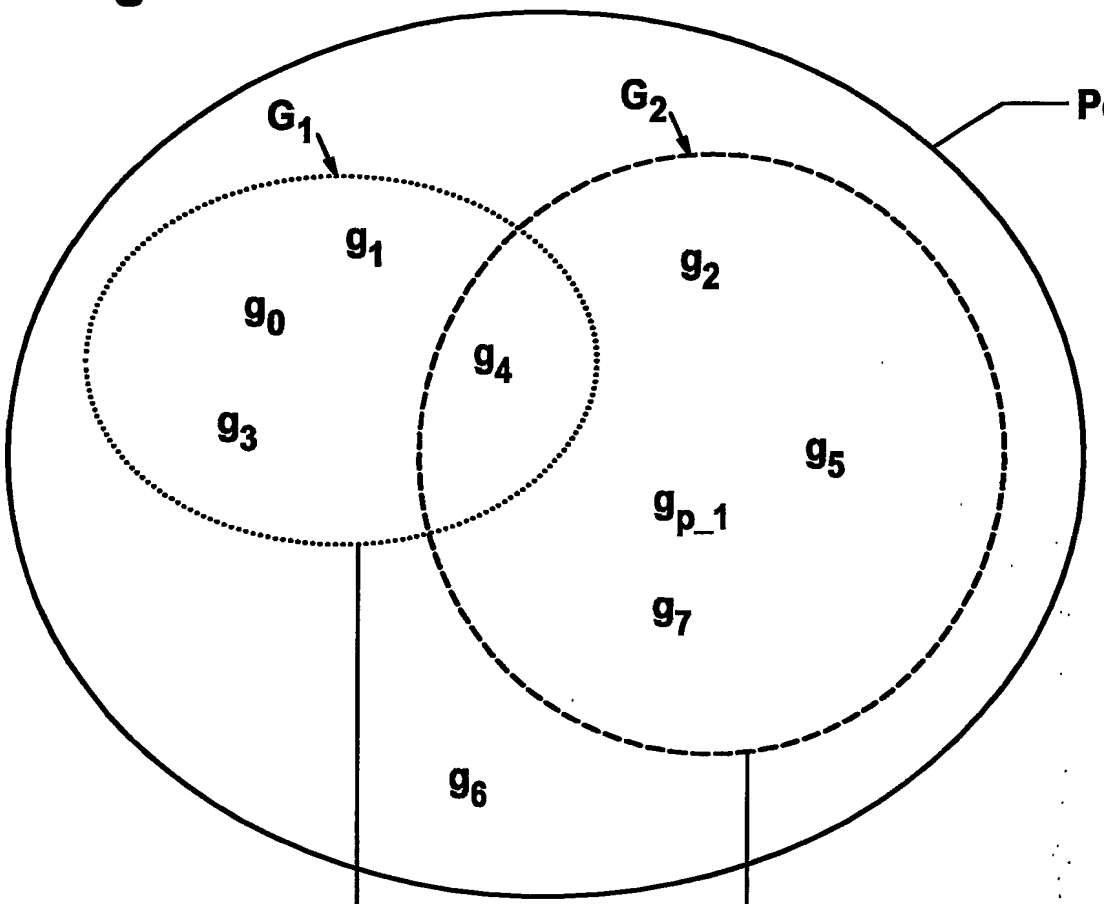

Verbindungsaufbau
100
200
Festlegen einer Permutations - Funktion
210
Festlegen von Entschlüsselungs - Mustern
220
Festlegen eines Sprung - Intervalls
230
Dynamisches Entschlüsseln
300
400
n=1
410
Abwarten I hop
420
n++
430
Ja
n>M ?
440
Nein
v_n = g_(p_n)
450

Fig. 6



wenn F = {5, 4, 7, 2, 7},
dann v(t) = {g_5, g_4, g_7, g_2, g_7, g_5, g_4 ...}
oder, wenn F = {7, 4, p_1, 2, 5},
dann v(t) = {g_7, g_4, g_{p_1}, g_2, g_5, g_7 ...}

wenn F = {1, 3, 0, 4},
dann v(t) = {g_1, g_3, g_0, g_4, g_1, g_3, g_0 ...}
oder, wenn F = {4, 0, 3, 1},
dann v(t) = {g_4, g_0, g_3, g_1, g_4, g_0 ...}